Załącznik nr 4

do Zarządzenia nr 5/2021
Przewodniczącego Zarządu Związku
Gmin Krajny
z dnia 2 listopada 2021 r.

INSTRUKCJA ZARZĄDZANIA

SYSTEMEM INFORMATYCZNYM

służącym do przetwarzania danych osobowych

Administrator Danych Osobowych *- Związek Gmin Krajny w Złotowie, ul. Wawrzyniaka 4a, 77-400 Złotów*

Instytucja objęta dokumentem*:*
Związek Gmin Krajny w Złotowie, ul. Wawrzyniaka 4a, 77-400 Złotów

Spis treści:

1. CEL INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Celem niniejszego dokumentu jest określenie zasad właściwego zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać wchodzące w jego skład urządzenia, odpowiednio do skali zagrożeń i kategorii danych objętych ochroną.

Stosowanie zasad określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez **INSTYTUCJĘ** w systemach informatycznych rozumiane jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

2. ŹRÓDŁA WYMAGAŃ

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją" została opracowana zgodnie z wymogami:
Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (RODO) art. 24;
USTAWA o ochronie danych osobowych z dnia 10 maja 2018 r. (t.j. Dz. U. z 2019 r. poz. 1781)

3. ZAKRES STOSOWANIA

Instrukcję stosuje się do danych osobowych przetwarzanych w systemach informatycznych, danych osobowych zapisanych w postaci elektronicznej na zewnętrznych nośnikach informacji oraz informacji dotyczących bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych.

Instrukcja zawiera specyfikację podstawowych środków technicznych ochrony danych osobowych oraz elementów zarządzania systemem informatycznym. W przypadku wystąpienia potrzeb wprowadzenia nowych lub modyfikacji istniejących zasad bezpieczeństwa przetwarzania danych osobowych w systemie, wnioski o ich uwzględnienie i wdrożenie powinni składać właściwi przedstawiciele komórek organizacyjnych, w których przetwarzane są dane osobowe, bezpośrednio do Administratora Systemów Informatycznych (ASI).

Niniejsza instrukcja znajduje zastosowanie do systemów informatycznych, stosowanych w **INSTYTUCJI**, w której przetwarzane są dane osobowe, a w szczególności określa:

a) zasady dotyczące bezpieczeństwa systemów informatycznych;

b) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w Systemie Informatycznym;

c) metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

d) procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników Systemu;

e) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

f) sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych;

g) zarządzanie bezpieczeństwem sieci;

h) sposób zabezpieczenia Systemu Informatycznego przed działalnością wirusów komputerowych, nieuprawnionym dostępem oraz awariami zasilania;

i) sposoby realizacji w Systemie wymogów dotyczących przetwarzania danych;

j) procedury wykonywania przeglądów i konserwacji Systemu oraz nośników informacji służących do przetwarzania danych.

Przyjęta przez Administratora do stosowania, stanowi obowiązujący wszystkich pracowników i współpracowników dokument.

4. DEFINICJE

4.1. Administrator Danych Osobowych ADO decyduje o środkach i celach przetwarzania danych osobowych.

4.2. Administrator Systemów Informatycznych (ASI) – rozumie się przez to osobę wyznaczoną przez Administratora Danych Osobowych, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych, w których przetwarzane są dane osobowe.

4.3. Dane osobowe – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

4.4. Osoba upoważniona – osoba posiadająca formalne upoważnienie wydane przez Administratora danych lub przez osobę wyznaczoną, uprawniona do przetwarzania danych osobowych.

4.5. Przetwarzanie danych osobowych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

4.6. System informatyczny – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

4.7. Użytkownik systemu – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym.

4.8. Zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.

4.9 Ilekroć w niniejszej polityce bezpieczeństwa jest mowa o:

Integralności - należy przez to rozumieć zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieuprawniony.

Poufności - należy przez to rozumieć zapewnienie, że informacja nie jest udostępniana lub ujawniana podmiotom nieuprawnionym.

Dostępności - należy przez to rozumieć zapewnienie, że dane są możliwe do wykorzystania zawsze, gdy podmiot uprawniony tego potrzebuje.

Rozliczalności - należy przez to rozumieć zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

5. ODPOWIEDZIALNOŚĆ

5.1. Administrator Systemu Informatycznego (ASI) – obowiązki podstawowe

1. Zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa.
2. Doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem.
3. Przydziela identyfikatory (loginy) użytkownikom systemu Informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu.
4. Nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu.
5. Zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych.
6. Prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

5.2. Administrator Systemu Informatycznego (ASI) – obowiązki szczegółowe

Do obowiązków Administratora Systemu Informatycznego, należy nadzorowanie przestrzegania zasad ochrony danych osobowych w systemach informatycznych. Do obowiązków w tym zakresie należą:

1) nadzór nad stosowaniem środków ochrony w systemach informatycznych;
2) nadzór nad przestrzeganiem przez administratorów i użytkowników systemu procedur bezpieczeństwa;
3) uzgadnianie z ADO szczególnych procedur regulujących wykonywanie czynności w systemach lub aplikacjach służących do przetwarzania danych osobowych;
4) zapewnienie doradztwa w zakresie przestrzegania przez pracowników firm zewnętrznych zasad ochrony danych osobowych przyjętych w Urzędzie.

Do obowiązków Administratora Systemu Informatycznego należy bieżąca ocena bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych, identyfikacja podatności na zagrożenia bezpieczeństwa przetwarzania danych osobowych oraz bezpieczne zarządzanie systemami. Do obowiązków w tym zakresie należą:

1) zarządzanie kontrolą dostępu do systemów informatycznych;
2) weryfikacja zdarzeń systemowych;
3) zarządzanie kontami użytkowników;
4) wdrażanie mechanizmów bezpieczeństwa przetwarzania danych osobowych;
5) kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym;
6) regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania tych kopii zapasowych.

5.3. Użytkownicy systemu

Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej. Do obowiązków należy również:

1) współpraca przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu;
2) przestrzeganie opracowanych dla systemu zasad przetwarzania danych osobowych oraz procedur i instrukcji;
3) informowanie ADO o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych;
4) wykonywania bez zbędnej zwłoki poleceń ADO w zakresie ochrony danych osobowych jeśli są one zgodne z przepisami prawa powszechnie obowiązującego;
5) stosowanie się do zaleceń zawartych w „Regulaminie użytkownika systemu informatycznego” – **ZAŁĄCZNIK NR 1**.

6. ZARZĄDZANIE BEZPIECZEŃSTWEM SYSTEMÓW

6.1. Podstawowe cele zabezpieczeń danych

6.1.1. Podstawowym celem zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych jest zapewnienie jak najwyższego poziomu bezpieczeństwa tych danych, które są w nich przetwarzane.

6.1.2. W celu zachowania odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych, dostęp do systemu informatycznego przetwarzającego dane osobowe powinien być możliwy wyłącznie po podaniu identyfikatora odrębnego dla każdego użytkownika systemu i poufnego hasła lub innego elementu uwierzytelniającego.

6.2. Podstawowe zasady zabezpieczeń systemów

6.2.1. Należy zapewnić poufność, integralność i rozliczalność systemów informatycznych służących do przetwarzania danych osobowych.

6.2.2. Należy zapewnić aby użytkownicy systemów informatycznych służących do przetwarzania danych osobowych nie posiadali wyższych poziomów uprawnień w tych systemach niż wymagane do wykonywania powierzonych obowiązków.

6.2.3. Należy zapewnić aby wszelkie działania użytkowników systemów informatycznych zapewniały rozliczalność tych działań.

6.3. Prawidłowy poziom zabezpieczeń danych

Prawidłowy poziom zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych zostaje zapewniony poprzez przestrzeganie następujących zasad:

1) uniemożliwienie osobom postronnym uzyskiwania nieupoważnionego dostępu do systemu;
2) instalowanie nowego lub aktualizowanie już zainstalowanego oprogramowania wyłącznie przez uprawnionych użytkowników systemu (ASI);
3) niepodejmowanie przez użytkowników systemu prób testowania, modyfikacji i naruszenia zabezpieczeń systemu lub jakichkolwiek działań noszących takie znamiona.

7. BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH

7.1. Wymagania bezpieczeństwa

7.1.1. Bezpieczeństwo powinno być integralną częścią systemów informatycznych służących do przetwarzania danych osobowych.

7.1.2. Usługi oraz aplikacje, które nie są wykorzystywane powinny być wyłączone.

7.1.3. Krytyczne poprawki bezpieczeństwa powinny być przetestowane i zainstalowane.

7.1.4. Dostęp do poszczególnych usług systemów informatycznych powinien być chroniony kontrolą dostępu.

7.1.5. Do systemów istotnych dla funkcjonowania Urzędu powinno być zapewnione wsparcie techniczne producentów. W miarę możliwości należy ograniczać liczbę elementów systemu informatycznego, dla których brak wsparcia mógłby stanowić o obniżeniu bezpieczeństwa. Użytkowanie systemów informatycznych bez wsparcia producenta jest dopuszczalne, o ile ich stosowanie nie wpływa znacząco na poziom bezpieczeństwa.

7.2. Bezpieczeństwo fizyczne i środowiskowe

7.2.1. Tylko uprawnieni pracownicy mają dostęp do pomieszczeń, w których są ulokowane kluczowe elementy infrastruktury (np. serwerowni). Rejestr osób upoważnionych do przebywania w tych pomieszczeniach prowadzi ABI.

7.2.2. Pomieszczenia, w których są ulokowane kluczowe elementy infrastruktury powinny być zamknięte i chronione przed dostępem osób postronnych.

7.2.3. Pomieszczenie serwerowni powinno być wyposażone w odpowiednie systemy – zgodnie z przepisami prawa – przepisami bezpieczeństwa i ochrony pożarowej.

7.2.4. Serwery powinny być podłączone do urządzeń awaryjnego podtrzymania zasilania (UPS).

7.2.5. W pomieszczeniach, w których są ulokowane kluczowe elementy infrastruktury nie powinno się przechowywać elementów łatwopalnych. Pomieszczenia te powinny być wyposażone w sprzęt gaśniczy.

7.3. Zarządzanie systemami informatycznymi

7.3.1. Konto administratora systemu informatycznego (konto mające najwyższe uprawnienia) powinno być używane tylko w uzasadnionych przypadkach. Do codziennej pracy należy używać kont o niższych uprawnieniach.

7.3.2. Administrator Systemu Informatycznego powinien odnotowywać w prowadzonych rejestrach systemów wszystkie ważne zdarzenia związane z zarządzanym systemem, w szczególności:

1) zmiany, np. instalacja nowego oprogramowania;
2) fakty wejścia do serwerowni osób trzecich;
3) okresowe testy i konserwacje;
4) incydenty bezpieczeństwa (awarie sprzętu, błędy oprogramowania, naruszenia bezpieczeństwa, zdarzenia losowe, ataki szkodliwego oprogramowania) i sposób ich obsługi;
5) fakty audytowania i kontroli.

7.4. Dokumentacja systemów

7.4.1. Należy prowadzić dokumentację eksploatowanych systemów informatycznych w celu zapewnienia oczekiwanej funkcjonalności, jakości, dostępności i bezpieczeństwa systemów.

7.4.2. Dokumentacja systemów powinna być aktualizowana na bieżąco, a dostęp do niej ograniczony dla uprawnionych osób na zasadzie wiedzy koniecznej.

7.4.3. Poziom szczegółowości dokumentacji powinien być adekwatny do tego, jak istotną rolę pełni dany element systemu informatycznego.

Dokumentacja powinna pozwalać na:

1) lokalizację awarii i usunięcie jej przyczyn,
2) odtworzenie systemu informatycznego po awarii,
3) konfigurację nowych urządzeń (np. routerów, przełączników sieciowych itd.),
4) przeprowadzenie analizy bezpieczeństwa i optymalizacji systemu informatycznego.

7.4.4. Dokumentację systemów informatycznych można prowadzić w formie elektronicznej. Należy w sposób jednoznaczny oznaczać dokumentację w celu określenia jej aktualności.

7.4.5. Dokumentacja przeznaczona dla użytkowników danego programu bądź systemu (instrukcje użytkownika) powinna być dostępna dla jego użytkowników.

7.5. Inwentaryzacja sprzętu i oprogramowania

Należy prowadzić ewidencję sprzętu i oprogramowania. Ewidencja ta może być prowadzona przy pomocy wyspecjalizowanego oprogramowania usprawniającego jej prowadzenie. System taki powinien na bieżąco aktualizować takie wykazy i na żądanie wygenerować odpowiednie raporty zawierające informacje o zainstalowanym sprzęcie informatycznym i oprogramowaniu.

7.6. Szkolenia

Użytkownicy systemu powinni podlegać okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (np. wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

8. KONTROLA DOSTĘPU

8.1. Kontrola dostępu do danych

8.1.1. Należy zapobiegać nieautoryzowanemu i nieuprawnionemu dostępowi do systemów informatycznych służących do przetwarzania danych osobowych.

8.1.2. Wszelkie czynności mogące powodować nieuprawniony dostęp do systemów informatycznych są zabronione.

8.1.3. Dane osobowe przechowywane na urządzeniach mobilnych takich jak np. komputerach przenośnych, tabletach, smartfonach, telefonach komórkowych powinny być zabezpieczone w sposób zapewniający poufność tym danym.

8.1.4. Serwery oraz stacje robocze należy tak skonfigurować, aby w przypadku nieaktywności użytkownika przez zdefiniowany okres (zalecane 10 minut) uruchamiał się wygaszasz ekranu odblokowywany hasłem.

8.2. Zarządzanie dostępem użytkowników

8.2.1. Dostęp do systemów informatycznych służących do przetwarzania danych osobowych należy zapewnić wyłącznie autoryzowanym użytkownikom na podstawie formalnych procedur przyznawania praw dostępu. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie. Upoważnienie nadaje ADO na podstawie wniosku o nadanie uprawnień do systemów sporządzonego przy współpracy z ASI. Konta dostępowe do systemów informatycznych przydziela ASI na wniosek ADO. Wzór **Wniosku o nadanie/modyfikację/odebranie uprawnień określa** – **ZAŁĄCZNIK NR 2**. ASI prowadzi i przechowuje w bezpiecznym miejscu **Rejestr uprawnień do systemów informatycznych** – **ZAŁĄCZNIK NR 3**.

8.2.2. Należy dokonać niezwłocznej zmiany praw dostępu użytkownikom, którzy zmienili stanowisko pracy lub obszar odpowiedzialności.

8.2.3. Należy dokonać niezwłocznego odebrania i zablokowania praw dostępu użytkownikom, którzy nie są już pracownikami lub którzy zakończyli świadczenie usług na podstawie umów, zamówień lub porozumień. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku: nieobecności użytkownika w pracy trwającej dłużej niż 30 dni kalendarzowych oraz zawieszenia w pełnieniu obowiązków służbowych.

8.2.4. Jeśli systemy informatyczne oferują taką funkcjonalność, to powinny automatycznie blokować użytkowników po określonej liczbie nieudanych prób uwierzytelniania (zalecana wartość: maksymalnie 5 prób).

8.2.5. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.

8.3. Identyfikacja użytkowników

8.3.1. Należy zapewnić aby każdy użytkownik posiadał unikalny identyfikator wyłącznie do swojego osobistego użytku, wygenerowany zgodnie z przyjętą konwencją nazewnictwa. Przyjmuje się, że identyfikator jest tworzony z pierwszej litery imienia, a po kropce nazwisko w pełnym brzmieniu, bez znaków polskich i pisanych małymi literami.

8.3.2. Wykorzystywanie identyfikatorów grupowych powinno być dozwolone wyłącznie w uzasadnionych przypadkach i powinno być udokumentowane oraz zatwierdzone.

8.3.3. Nie należy przyznawać innym użytkownikom wykorzystanych wcześniej identyfikatorów.

8.3.4. Identyfikatorów nie należy usuwać. Identyfikatory (konta) osób, którym wycofano uprawnienia powinny zostać zablokowane.

8.3.5. Konta funkcyjne lub serwisowe należy oznaczyć i zapewnić ich łatwą identyfikację oraz powinny wygasać po określonym czasie.

8.3.6. Konta użytkowników, którzy nie są etatowymi pracownikami należy oznaczyć i zapewnić ich łatwą identyfikację oraz powinny wygasać po określonym czasie.

8.3.7. Wszystkie konta dostępowe (identyfikatory) do systemów informatycznych należy chronić hasłem lub innym bezpiecznym sposobem uwierzytelniania. Nie należy stosować kont dostępowych bez hasła.

8.3.8. Wszelkie konta typu „gość" należy usunąć lub zablokować.

8.4. Zarządzanie przywilejami

8.4.1. Konta użytkownika uprzywilejowanego należy oznaczyć, zapewnić ich łatwą identyfikację.

8.4.2. Wyłącznie czynności, które wymagają użycia uprawnień uprzywilejowanych należy wykonywać z konta posiadającego uprawnienia uprzywilejowane. Nie należy używać kont uprzywilejowanych do codziennej pracy o ile nie ma takiej konieczności.

8.4.3. Konta uprzywilejowane i ich uprawnienia należy okresowo przeglądać.

8.4.4. Czynności wykonywane za pomocą kont uprzywilejowanych należy rejestrować oraz zapewnić możliwości ich identyfikacji i rozliczalności.

8.5. Zarządzanie hasłami

8.5.1. Przydzielanie haseł powinno być kontrolowane za pośrednictwem formalnego procesu zarządzania. Hasła do systemów informatycznych przydziela ASI na wniosek ADO.

8.5.2. Hasła powinny być dobrej jakości:

1) długości co najmniej 8 znaków;
2) które są łatwe do zapamiętania, a trudne do odgadnięcia;
3) nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, numer telefonu, data urodzenia itp.);
4) w których występuje przynajmniej jedna duża litera, jedna mała litera, jedna cyfra i znak specjalny.

8.6. Zmiana haseł

8.6.1. Należy zapewnić aby hasła były regularnie zmieniane, okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła) oraz/lub w przypadku ujawnienia lub podejrzenia ujawnienia hasła.

8.6.2. W przypadku gdy dla danego systemu występuje wymaganie prawne związane ze zdefiniowaną częstotliwością zmiany hasła, należy przyjąć, że powinien on wymusić zmianę hasła co najmniej raz na 30 dni.

8.6.3. W przypadku gdy funkcjonalność danego systemu nie zapewnia automatycznego wymuszania zmiany haseł, należy zobligować użytkowników do samodzielnej zmiany haseł, zgodnie z zasadami przyjętymi dla danego systemu informatycznego.

8.6.4. Hasło początkowe, które jest przydzielane przez administratora systemu, powinno umożliwiać użytkownikowi zarejestrowanie się w systemie tylko jeden raz i powinno być natychmiast zmienione przez użytkownika systemu.

8.6.5. Hasła należy niezwłocznie zmieniać w przypadkach, gdy cokolwiek mogłoby wskazywać na możliwość naruszenia bezpieczeństwa systemu informatycznego lub hasła.

8.6.6. Należy zapewnić aby wszelkie urządzenia sprzętowe lub programowe, które na początku posiadały hasło domyślne, miały zmienione hasło zgodnie z przyjętymi wymogami dotyczącymi formułowania haseł.

8.6.7. Zaleca się, by systemy informatyczne przechowywały historię haseł oraz uniemożliwiały zastosowanie haseł, które były wcześniej używane przez danego użytkownika (zalecana historia 10 haseł).

8.7. Zabezpieczenie haseł

8.7.1. Hasła nie powinny być przechowywane w systemach, aplikacjach, bazach danych, skryptach i plikach konfiguracyjnych w postaci jawnej, bez zapewnienia im poufności.

8.7.2. Hasła nie powinny być przesyłane za pomocną narzędzi i usług teleinformatycznych w postaci jawnej, bez zapewnienia im poufności.

8.7.3. Należy stosować bezpieczną procedurę przekazywania haseł użytkownikom np. nieprzesyłanie przez sieć haseł (np. w niechronionych wiadomościach poczty elektronicznej).

8.7.4. Czynności związane z przechwytywaniem lub odgadywaniem haseł innych użytkowników są zabronione.

8.7.5. Hasła należy utrzymywać w tajemnicy również po upływie ich ważności.

8.7.6. Aktualne hasła administratora systemu są przechowywane w zamkniętej kopercie w sejfie ognioodpornym, do którego ma dostęp administrator systemu informatycznego oraz ADO.

8.8. Przegląd oraz weryfikacja kont i uprawnień

8.8.1. Wszystkie konta należy blokować po zdefiniowanym okresie bezczynności.

8.8.2. Przegląd kont i uprawnień należy przeprowadzać regularnie, co najmniej raz na 12 miesięcy.

8.8.3. Należy zapewnić niezwłoczne blokowanie zbędnych kont użytkowników oraz uprawnień.

8.8.4. Konto użytkownika należy zablokować po upływie zdefiniowanego okresu bezczynności (zalecane 60 dni od daty ostatniego użycia).

8.9. Odpowiedzialność użytkowników

8.9.1. Pierwsze zarejestrowanie użytkownika w systemie i nadanie odpowiednich uprawnień do systemu przetwarzającego dane osobowe musi być poprzedzone złożeniem przez użytkownika oświadczenia o zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczania oraz przetwarzaniu danych osobowych zgodnie z przepisami, a także uzyskaniem formalnego upoważnienia do przetwarzania danych osobowych.

8.9.2. Użytkownicy powinni zapobiegać utracie i zniszczeniu powierzonego sprzętu, naruszeniu bezpieczeństwa oraz nieuprawnionemu dostępowi do systemów informatycznych służących do przetwarzania danych osobowych.

8.9.3. Użytkownicy powinni być świadomi swojej odpowiedzialności za utrzymanie skutecznej kontroli dostępu, szczególnie w odniesieniu do haseł i zabezpieczenia swojego sprzętu.

8.9.4. Użytkownicy nie powinni stosować jednego hasła do wielu systemów informatycznych.

9. ROZPOCZĘCIE, ZAWIESZENIE I ZAKOŃCZENIE PRACY

9.1. Przed przystąpieniem do pracy z systemem informatycznym, użytkownik systemu zobowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

9.2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest powiadomić o tym fakcie swojego przełożonego lub ADO.

9.3. Kończąc pracę, użytkownik systemu obowiązany jest do wylogowania się z systemu informatycznego i zabezpieczenia stanowiska pracy, w szczególności wszelkiej dokumentacji, wydruków oraz elektronicznych nośników informacji, na których znajdują się dane osobowe i umieszczenia ich w zamykanych szafkach.

9.4. Stacje robocze powinny być tak skonfigurowane, aby w przypadku nieobecności użytkownika systemu dłużej niż 10 minut uruchamiał się wygaszasz ekranu odblokowywany hasłem. W przypadku chwilowego opuszczenia stanowiska pracy użytkownik powinien wylogować się z systemu lub zablokować stację roboczą. Odblokowanie jest możliwe po podaniu hasła.

10. BEZPIECZEŃSTWO DANYCH

10.1. Poufność

10.1.1. Dane osobowe zapisane w postaci elektronicznej należy przetwarzać wyłącznie na urządzeniach służbowych zabezpieczonych zgodnie z obowiązującymi procedurami.

10.1.2. Należy zapewnić aby wszelkie informacje o systemach informatycznych służących do przetwarzania danych osobowych, których ujawnienie może powodować utratę bezpieczeństwa tego systemu lub danych w nim przetwarzanych nie były ujawniane użytkownikom ani żadnej innej nieuprawnionej osobie, za wyjątkiem informacji niezbędnych do prawidłowego korzystania z tych systemów.

10.1.3. Użytkownicy systemów informatycznych służących do przetwarzania danych osobowych nie powinni ujawniać informacji o charakterze, funkcjonalności, zastosowanych środkach kontrolnych, sposobie ich obsługi oraz lokalizacji wykorzystywanych systemów osobom, które nie są uprawnione do otrzymania tego typu informacji.

10.1.4. Dane osobowe powinny być przetwarzane przy użyciu systemów informatycznych zgodnie z zasadą wiedzy koniecznej.

10.2. Kopie zapasowe

10.2.1. Wykaz systemów, których dane należy kopiować stanowi: **Rejestr tworzenia kopii** – **ZAŁĄCZNIK NR 4**.

10.2.2. Za tworzenie i przechowywanie kopii zapasowych oraz prowadzenie ewidencji wykonania kopii zapasowych odpowiedzialny jest ASI.

10.2.3. Kopie zapasowe systemów przetwarzających dane osobowe są codziennie zapisywane na nośniki zewnętrzne (inny nośnik każdego dnia). Zapis odbywa się w godzinach wieczornych.

10.2.4. Nośniki kopii zapasowych oznaczane są w sposób umożliwiający określenie daty utworzenia kopii oraz nazwy systemu.

10.2.5. Nośniki z kopiami zapasowymi przechowywane są w sejfie ogniotrwałym poza miejscem ich bieżącego przetwarzania. Dostęp do kopii bezpieczeństwa ma tylko ASI oraz ADO.

10.2.6. Utworzone kopie zapasowe podlegają weryfikacji ze względu na sprawdzenie możliwości odczytu danych.

10.2.7. Nieaktualne (nieprzydatne) kopie danych podlegają usunięciu. W przypadku nośników jednorazowych np. takich jak płyty CD, DVD itp. nośniki należy zniszczyć fizycznie w sposób uniemożliwiający odtworzenie zapisanych na nich danych.

Nośniki wielorazowego użytku, można ponownie wykorzystać do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości. Nośniki wielorazowego użytku , które nie nadają się do ponownego użycia należy zniszczyć fizycznie w sposób uniemożliwiający odtworzenie zapisanych na nich danych.

10.2.8. ASI odpowiedzialny jest za realizację działań odtworzeniowych w przypadku konieczności podjęcia takich działań w związku z awarią systemu informatycznego Urzędu. Po odtworzeniu systemu informatycznego ASI odpowiedzialny jest za przeprowadzenie testów poprawności działania systemu przed jego oddaniem do użytkowania.

10.2.9. ASI przeprowadza weryfikację możliwości odtworzenia wybranych danych zapisanych na kopiach zapasowych. Weryfikacja taka powinna być przeprowadzana nie rzadziej niż raz na pół roku.

10.3. Przechowywanie nośników elektronicznych

10.3.1. Wymienne nośniki elektroniczne i karty kryptograficzne, powinny być użytkowane i przechowywane przez pracowników w sposób minimalizujący ryzyko ich utraty, uszkodzenia lub zniszczenia (przechowywane w zamykanych meblach biurowych).

10.3.2. Dane przechowywane są na nośnikach przenośnych jedynie w przypadkach, gdy jest to konieczne, przez czas niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane. Po ustaniu potrzeby ich przechowywania, zawartość nośnika podlega skasowaniu w sposób uniemożliwiający odtworzenie danych, a w przypadku gdy nie jest to możliwe, takie nośniki należy zniszczyć w sposób uniemożliwiający odczytanie/odzyskanie danych osobowych.

10.3.3. W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe w tym dane wrażliwe, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność, integralność i rozliczalność tych danych, przez co rozumie się:

1) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi;
2) stosowanie metod kryptograficznych;
3) stosowanie odpowiednich zabezpieczeń fizycznych;
4) stosowanie odpowiednich zabezpieczeń organizacyjnych;
5) w zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.

10.3.4. Dane osobowe przetwarzane na komputerach przenośnych powinny być zabezpieczone w sposób zapewniający poufność tych danych, w szczególności dane te powinny być zabezpieczone metodami kryptograficznymi.

10.3.5. W przypadku wycofania sprzętu komputerowego z użycia, dane osobowe na nim zapisane są kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych. W przypadku braku możliwości programowego usunięcia danych nośnik podlega fizycznemu zniszczeniu. Za usunięcie danych odpowiada ASI.

Dopuszcza się powierzenie niszczenia nośników danych wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem:

1) Zawarcia stosownej umowy,
2) Zagwarantowania poufności danych przez usługodawcę,
3) Umożliwienie prowadzenia nadzoru nad procesem niszczenia nośników przez ABI lub ASI,
4) Udokumentowania faktu zniszczenia nośników protokołem.

10.4. Zasady postępowania z komputerami przenośnymi

10.4.1. Osoba używająca komputer przenośny zawierający dane osobowe zobowiązana jest zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych.

10.4.2. Osoba używająca komputer przenośny zawierający dane osobowe w szczególności powinna:

1) stosować ochronę kryptograficzną wobec danych osobowych przetwarzanych na komputerze przenośnym;
2) zabezpieczyć dostęp do komputera na poziomie biosu i systemu operacyjnego - identyfikator i hasło;
3) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych;
4) nie wykorzystywać komputera przenośnego do przetwarzania danych osobowych w obszarach użyteczności publicznej;
5) zachować szczególną ostrożność przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych.

10.4.3. W przypadku podłączania komputera przenośnego do sieci publicznej poza siecią ADO należy zastosować firewall zainstalowany bezpośrednio na tym komputerze oraz system antywirusowy.

10.4.4. Użytkownik powinien zachować wyjątkową ostrożność podczas korzystania z zasobów sieci publicznej.

10.4.5. Zabrania się wynoszenia komputerów przenośnych poza obszar Urzędu, jeśli zawierają one dane osobowe.

10.5. Zasady postępowania z nośnikami wymiennymi

10.5.1. Dopuszczone do użytku są jedynie zaewidencjonowane nośniki wymienne. Nie należy używać nośników prywatnych lub nośników niewiadomego pochodzenia.

10.5.2. Przed użyciem nośnik wymienny powinien zostać sprawdzony programem antywirusowym.

10.5.3. System informatyczny powinien rejestrować fakt użycia przez pracowników nośników wymiennych, nazw plików jakie są na taki nośnik zapisywane oraz z niego odczytywane.

10.5.4. Jeśli nośniki wymienne zawierają dane wrażliwe, przed opuszczeniem obszaru ich przetwarzania, należy je zabezpieczyć narzędziami kryptograficznymi.

10.5.5. Zaleca się, by nośniki wymienne wykorzystywane przez pracowników zawierały mechanizmy uniemożliwiające osobom nieuprawnionym dostęp do zapisanych danych.

10.6. Bezpieczeństwo wydruków

10.6.1. Umiejscowienie drukarek powinno uniemożliwiać przejęcie wydruków przez osoby postronne.

10.6.2. Informacje o wysokim stopniu poufności należy drukować na drukarkach podłączonych lokalnie do komputera.

10.6.3. Drukarki sieciowe powinny mieć zmienione domyślne hasła pozwalające na zarządzanie ustawieniami.

10.6.4. Przy sporządzaniu wydruków na drukarkach sieciowych należy zachować ostrożność podczas wyboru drukarki, na której mają zostać wydrukowane dokumenty, aby wydruk nie dostał się do osób nieupoważnionych.

10.6.5. Wydruki należy niezwłocznie odebrać, aby wydrukowane dokumenty nie leżały na podajnikach.

10.6.6. W przypadku, gdy wydruk zablokuje się w kolejce wydruku nie należy wykonywać kolejnych wydruków, jeśli poprzedni wydruk się nie powiódł.

10.7. Przesyłanie danych poza obszar przetwarzania

10.7.1. Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez zastosowanie ochrony kryptograficznej.

10.7.2. W wypadku przesyłania danych osobowych przez sieć internetową pocztą elektroniczną należy każdy z załączników zabezpieczyć ochroną kryptograficzną poprzez nadanie hasła odczytu. Hasło należy przesłać lub podać odbiorcy z wykorzystaniem innych metod komunikacji (tel., faks, bezpośrednia rozmowa).

10.7.3. Zabrania się przekazywania danych przez aplikacje internetowe nie wykorzystujące odpowiedniego protokołu szyfrowania (adres internetowy musi być poprzedzony zapisem „https”).

11. ZARZĄDZANIE BEZPIECZEŃSTWEM SIECI

11.1. Podstawowe zasady

11.1.1. Należy zapewnić, że infrastruktura sieciowa jest właściwie chroniona, adekwatnie do zagrożeń mogących powodować utratę bezpieczeństwa przetwarzania danych osobowych. Elementy sieci komputerowej (routery, przełączniki, gniazda sieciowe itp.) nie mogą być dostępne dla osób postronnych.

11.1.2. Dane osobowe przesyłane poprzez publiczną sieć telekomunikacyjną powinny być zabezpieczone środkami kryptograficznej ochrony.

11.1.3. ASI powinien chronić system przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, poprzez: kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną; kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.

11.1.4. Wewnętrzna adresacja IP, konfiguracja oraz informacja o systemach powiązanych nie powinna być ujawniana osobom nieuprawnionym.

11.1.5. Podłączanie do infrastruktury sieciowej nieautoryzowanych urządzeń takich jak modemy, urządzenia sieciowe, w tym urządzenia sieci bezprzewodowych jest zabronione.

11.1.6. Podłączanie we własnym zakresie stacji roboczych do publicznej sieci telekomunikacyjnej poprzez nieautoryzowane urządzenia sieciowe, będąc jednocześnie podłączonym do infrastruktury lokalnej LAN powinno być zabronione.

11.1.7. Należy zastosować specjalne zabezpieczenia (np. kryptograficzne środki ochrony) w celu ochrony integralności i poufności danych przesyłanych przez sieci bezprzewodowe.

11.2. Sieć rozległa (WAN) – usługi internetowe oraz zdalny dostęp

11.2.1. Usługi udostępniane w sieci Internet powinny być wydzielone do strefy DMZ oraz być zinwentaryzowane.

11.2.2. Usługi udostępniane w sieci Internet oraz ruch wchodzący powinny być ograniczone do niezbędnego minimum.

11.2.3. Należy regularnie badać usługi udostępniane w sieci Internet pod kątem występowania luk bezpieczeństwa. Należy zapewnić aktualność stosowanego na serwerach oprogramowania.

11.2.4. Wykorzystywanie zasobów serwera plików w sieci publicznej (Internecie) jest zabronione. Dostęp użytkowników zdalnych do zasobów systemu informatycznego Urzędu jest możliwy wyłącznie za pomocą tuneli VPN.

11.2.5. W przypadku wykorzystywania pracy na odległość (zdalnego dostępu), należy stosować tunele VPN zabezpieczone przy użyciu silnych algorytmów szyfrujących oraz dwustopniowym uwierzytelnianiem (np. hasło dostępowe oraz losowy kod przesyłany na podany wcześniej adres email).

11.2.6. Należy wprowadzić system IDS/IPS w miejscach narażonych na ryzyko włamania sieciowego (np. na styku sieci WAN i sieci lokalnej). Miejsca takie należy objąć monitorowaniem.

11.2.7. Należy zapewnić ważność licencji w systemie IDS/IPS. Zaleca się, by urządzenia te posiadały wsparcie techniczne.

11.3. Sieć lokalna (LAN)

11.3.1. Zaleca się, by gniazda sieciowe były zabezpieczone fizycznie i logicznie przed podłączeniem obcych urządzeń do infrastruktury Urzędu. Zaleca się, by przełączniki sieciowe były zabezpieczone przed nieuprawnionym dostępem.

11.3.2. Jeśli gniazda sieciowe są dostępne publicznie, należy zastosować mechanizmy uniemożliwiające nieautoryzowany dostęp do sieci LAN.

11.3.3. Zaleca się wprowadzenie mechanizmów zabezpieczających możliwość podłączenia do sieci tylko autoryzowanych (służbowych) urządzeń. W przypadku potrzeby krótkotrwałego przyznania osobom postronnym dostępu do sieci Internet, należy takie połączenie zrealizować za pomocą wydzielonego od reszty segmentu sieci (np. VLAN).

11.3.4. W przypadku podłączenia nowego urządzenia do sieci lokalnej należy upewnić się, że nie nastąpi konflikt adresów IP z istniejącym urządzeniem.

11.3.5. Nie należy pozostawiać domyślnych ustawień na urządzeniach sieciowych.

11.4. Polityka dotycząca korzystania z usług sieciowych

11.4.1. Użytkownikom należy zapewnić dostęp tylko do tych usług infrastruktury teleinformatycznej (np. dostęp do Internetu, zdalny dostęp, poczta elektroniczna) do których zostali autoryzowani.

11.4.2. Należy zapewnić, że osoby nie będące pracownikami nie posiadają nieautoryzowanego i niekontrolowanego dostępu do infrastruktury teleinformatycznej.

11.4.3. Należy zapewnić, że niezabezpieczone usługi infrastruktury teleinformatycznej, pozwalające przesyłać hasła w postaci niezabezpieczonej np. telnet lub ftp, nie są wykorzystywane i są zablokowane.

11.5. Bezpieczeństwo sieci bezprzewodowych

11.5.1. Sieci bezprzewodowe podłączone do infrastruktury teleinformatycznej powinny być autoryzowane, udokumentowane, monitorowane oraz odpowiednio zabezpieczone. Należy w miarę możliwości:

1) zrezygnować z używania sieci bezprzewodowych jeśli jest możliwość zastosowania połączenia przewodowego,
2) odseparować ruch z sieci bezprzewodowych do pozostałych segmentów sieci,
3) zmniejszyć siłę sygnału radiowego,
4) zmienić standardową nazwę sieci (SSID) i wyłączyć jej rozgłaszanie.

11.5.2. Wszystkie urządzenia sieci bezprzewodowych podłączone do infrastruktury informatycznej powinny wykorzystywać bezpieczne protokoły komunikacyjne z zaawansowaną funkcją szyfrowania i uwierzytelniania. Zaleca się okresową zmianę kluczy szyfrujących, np. raz na kwartał.

11.6. Polityka dotycząca korzystania z Internetu

11.6.1. Wykonywane połączenia do Internetu powinny być monitorowane i rejestrowane.

11.6.2. Systemy monitorowania połączeń do Internetu powinny rejestrować źródłowy adres IP, datę i godzinę połączenia, wykorzystywany protokół, docelową witrynę lub urządzenie (adres IP) oraz nazwę użytkownika nawiązującego połączenie.

11.6.3. Dostęp do Internetu powinien być zabezpieczony poprzez zastosowanie narzędzi służących do blokowania stron internetowych lub usług zawierających niepożądane treści lub zawartość, np. takie jak: materiały o charakterze pornograficznym, nielegalnym, obraźliwym, szkodliwe oprogramowanie oraz usługi udostępniania plików.

11.6.4. Wszystkie pliki ściągnięte z Internetu powinny być sprawdzane przez system antywirusowy.

11.6.5. Użytkownicy powinni być uświadamiani o zagrożeniach występujących podczas korzystania z Internetu.

11.6.6. Użytkownicy nie powinni otwierać żadnych plików i instalować żadnego oprogramowania ściągniętego z Internetu bez upewniania się czy został on ściągnięty z zaufanej strony oraz czy nie zagraża bezpieczeństwu systemów informatycznych.

11.7. Polityka dotycząca korzystania z poczty elektronicznej

11.7.1. Konta poczty elektronicznej zakłada ASI na wniosek ADO.

11.7.2. Administrator Systemu Informatycznego prowadzi rejestr kont poczty elektronicznej.

11.7.3. Administrator Systemu Informatycznego dokonuje blokady lub usunięcia nieaktualnych kont poczty elektronicznej w uzgodnieniu z Administratorem Danych Osobowych. Jeżeli istnieje potrzeba utrzymania ważności kont poczty elektronicznej stosowanych przez osoby, które nie są już pracownikami Urzędu lub przestały pełnić swoje funkcje, należy niezwłocznie zmienić hasła dostępowe.

11.7.4. Należy unikać stosowania kont poczty elektronicznej współdzielonych przez wiele osób.

11.7.5. Konta poczty elektronicznej powinny być zabezpieczone silnymi hasłami, a połączenia z serwerami poczty powinny być dokonywane przy użyciu bezpiecznych protokołów. W hasłach należy unikać fraz łatwych do odgadnięcia, np. znanych słów, imion, dat urodzenia itp. Nie należy używać tego samego hasła do różnych kont.

11.7.6. Należy zapewnić świadomość użytkowników, że poczta elektroniczna nie może być wykorzystywana do przesyłania informacji zawierających treści obraźliwe, szkodliwe, nielegalne, pornograficzne, dotyczących przekonań politycznych i uprzedzeń rasowych.

11.7.7. Wykorzystywanie prywatnych skrzynek pocztowych do przesyłania informacji służbowych jest niedozwolone.

11.7.8. Przychodzące i wychodzące wiadomości poczty elektronicznej należy sprawdzać na wypadek występowania wirusów i kodów złośliwych a potencjalne niebezpieczne załączniki należy blokować.

11.7.9. Wiadomości poczty elektronicznej otrzymane z nieznanych i podejrzanych źródeł nie powinny być otwierane i przekazywane dalej. W razie wątpliwości należy sprawdzić nagłówek wiadomości.

11.7.10. Nie należy wykorzystywać służbowej poczty elektronicznej do celów prywatnych.

12. SZKODLIWE OPROGRAMOWANIE

Podstawowe zasady

12.1. Systemy informatyczne należy chronić przed szkodliwym oprogramowaniem (np. wirusy, trojany, bomby logiczne, robaki) poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, m. in. poprzez:

1) oprogramowanie antywirusowe sprawujące ciągły nadzór nad pracą systemu informatycznego (praca w tle),
2) zaporę sieciową wraz z systemem antywirusowym, systemem IPS na styku sieci LAN Urzędu i Internetu,
3) aktualizację oprogramowania systemowego,
4) konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa.

12.2. Oprogramowanie antywirusowe należy aktywować na wszystkich serwerach, stacjach roboczych oraz na stacjach roboczych i serwerach połączonych za pomocą zdalnego dostępu.

12.3. Zastosowane zabezpieczenia ochrony antywirusowej powinny być adekwatne dla danego zasobu teleinformatycznego lub usługi.

12.4. Oprogramowanie antywirusowe powinno być zainstalowane tak aby użytkownik systemu nie był w stanie go wyłączyć lub pominąć etapu skanowania.

12.5. Kontrola antywirusowa powinna być przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.

12.6. Niezależnie od ciągłego nadzoru oprogramowania antywirusowego pracującego w tle, ASI okresowo dokonuje pełnego sprawdzenia pod kątem obecności wirusów na stacjach roboczych.

12.7. Aktualizacja sygnatur szkodliwego oprogramowania powinna być prowadzona automatycznie. Jeżeli automatyczna dystrybucja nowych sygnatur szkodliwego oprogramowania nie jest możliwa, powinna być prowadzona manualnie, co najmniej raz na tydzień.

13. PRACE SERWISOWE

Zasady wykonywania prac serwisowych, przeglądu i konserwacji systemów komputerowych oraz nośników informacji służących do przetwarzania danych osobowych

13.1. Przegląd i konserwacja sprzętu informatycznego realizowane są przez upoważnionych pracowników Urzędu oraz przez podmioty zewnętrzne. Osoby nie będące pracownikami, które prowadzą prace serwisowe na rzecz ADO przed rozpoczęciem prac, powinny być poddane weryfikacji tożsamości przez Administratora Systemu Informatycznego lub inną wyznaczoną do tego celu osobę.

13.2. Prace serwisowe wykonywane na terenie Urzędu przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi Administratora Systemu Informatycznego lub innej wyznaczonej osoby.

13.3. W przypadku gdy konieczne jest dokonanie przeglądu, naprawy lub konserwacji sprzętu informatycznego zawierającego dane osobowe, z urządzenia należy wymontować element, na którym zapisane są dane osobowe, o ile jest to możliwe. Przekazanie sprzętu teleinformatycznego do naprawy poza teren Urzędu jest dopuszczalne, jeżeli spełnione zostaną poniższe warunki:

1) sprzęt przekazywany jest bez nośników zawierających dane osobowe,
2) przekazanie sprzętu potwierdzane jest protokołem, pozwalającym na jednoznaczne wskazanie osoby przekazującej oraz osoby i firmy odbierającej sprzęt. Protokoły lub ich kopie przechowuje ASI.

W wypadku konieczności naprawy lub konserwacji sprzętu teleinformatycznego Urzędu poza miejscem jego użytkowania, kiedy nie można usunąć z naprawianego sprzętu danych osobowych, należy zawrzeć z podmiotem dokonującym naprawy umowę powierzenia w rozumieniu art. 31 ustawy o ochronie danych osobowych lub odstąpić od naprawy.

W przypadku uszkodzenia i wymiany gwarancyjnej sprzętu informatycznego zawierającego dane osobowe, należy skutecznie usunąć z niego dane osobowe (np. przez wielokrotne nadpisanie) lub wymontować element, na którym zapisane są dane osobowe. Jeśli to nie jest możliwe, należy odstąpić od naprawy / wymiany.

13.4. Wszelkie prace serwisowe dotyczące systemu informatycznego, wykonywane przez podmioty zewnętrzne (w tym wykonywane zdalnie w zakresie użytkowanego oprogramowania) wymagają zgody ASI przed rozpoczęciem prac oraz sporządzenia protokołu serwisowego, zawierającego co najmniej poniższe informacje:

1) wskazanie osoby przeprowadzającej prace serwisowe oraz podmiotu, którego osoba ta jest pracownikiem,
2) wskazanie osoby nadzorującej przebieg prac serwisowych (dotyczy sytuacji, gdy prace realizowane są w siedzibie Urzędu),
3) przedmiot prac serwisowych (w szczególności identyfikator sprzętu w przypadku prac serwisowych dotyczących sprzętu),
4) zakres prac serwisowych i ich wynik,
5) datę i czas przeprowadzania prac serwisowych.

14. WPROWADZANIE NOWYCH KOMPONENTÓW SYSTEMU INFORMATYCZNEGO

14.1. Zasady doboru elementów systemu informatycznego

14.1.1. Decyzję o potrzebie wprowadzenia nowego elementu systemu informatycznego i jego doborze podejmuje Administrator Systemu Informatycznego. Podejmując ją należy uwzględnić przeznaczenie danego elementu, korzyści jakie przyniesie jego zastosowanie oraz czy wprowadzenie danego komponentu systemu informatycznego nie obniży poziomu bezpieczeństwa systemu informatycznego.

Jeśli nowy element systemu informatycznego ma wpływ na bezpieczeństwo systemu informatycznego Administrator Systemu Informatycznego swoją decyzję konsultuje z ADO.

14.2. Weryfikacja ustawień

Przed wdrożeniem nowego elementu systemu informatycznego należy zweryfikować, czy nie pozostawiono domyślnych ustawień konfiguracyjnych (ustawień fabrycznych) , domyślnych haseł dostępowych itp.

14.3. Standardy konfiguracyjne

14.3.1. Należy rozważyć zasadność wprowadzenia standardów konfiguracyjnych. Jeżeli można zidentyfikować elementy systemu informatycznego o zbliżonych właściwościach, zaleca się wprowadzenie standardów konfiguracyjnych.

14.3.2. Standardy konfiguracyjne dotyczące systemu informatycznego określa Administrator Systemu Informatycznego biorąc pod uwagę funkcjonalność wybranych rozwiązań oraz ich wpływ na bezpieczeństwo systemu.

15. WPROWADZANIE ZMIAN W SYSTEMIE INFORMATYCZNYM

Zasady wprowadzania zmian do systemu informatycznego

15.1. Decyzje o zmianach w systemie informatycznym podejmuje Administrator Systemu Informatycznego w porozumieniu z Administratorem Danych Osobowych.

15.2. Zmiany w systemie informatycznym należy wprowadzać w sposób zaplanowany i kontrolowany, uwzględniając wpływ wprowadzanej zmiany na pozostałe elementy systemu informatycznego.

15.3. Przed wprowadzeniem zmiany należy zapewnić możliwość wycofania zmiany (np. kopie zapasowe danych, kopie konfiguracji itd.)

15.4. Zmiany w systemie informatycznym wprowadza Administrator Systemu Informatycznego.

15.5. Elementy systemu informatycznego powinny być zabezpieczone przed wprowadzaniem zmian w konfiguracji przez osoby nieuprawnione.

15.6. Zaleca się, by przed wprowadzeniem zmiany elementu systemu informatycznego, przetestować jego działanie w wydzielonym środowisku.

15.7. Usługi dostarczane przez strony trzecie wymagają przed wdrożeniem przetestowania i akceptacji, uwzględniając ich wpływ na bezpieczeństwo systemu informatycznego.

16. WYCOFYWANIE KOMPONENTÓW SYSTEMU INFORMATYCZNEGO

16.1. Zasady

16.1.1. Informację o potrzebie wycofania systemu lub sprzętu teleinformatycznego z użytku użytkownicy przekazują do Administratora Systemu Informatycznego.

16.1.2. Administrator Systemu Informatycznego dokonuje oceny przydatności danego systemu lub sprzętu komputerowego do wykorzystania w przyszłości i podejmuje decyzję o jego wycofaniu z użytku. W przypadku możliwości wykorzystania wycofywanego sprzętu lub oprogramowania na innym stanowisku, należy przeznaczyć je do dalszego wykorzystania.

16.1.3. W przypadku uzasadnionej ekonomicznie naprawy czy modernizacji sprzętu, należy po dokonanej naprawie / modernizacji taki sprzęt przeznaczyć do dalszego wykorzystania.

16.2. Wycofywanie sprzętu komputerowego z użytku

16.2.1. Sprzęt komputerowy przeznaczony do wycofania powinien być przechowywany w sposób zapewniający poufność danych a pomieszczenia, gdzie jest on składowany zamykane przed dostępem osób nieupoważnionych.

16.2.2. W przypadku komponentów sieci komputerowych, jeśli to potrzebne, sporządzić kopię ich konfiguracji. Następnie dane konfiguracyjne należy z urządzeń przeznaczonych do utylizacji usunąć.

16.2.3. Przed wycofaniem sprzętu informatycznego z użytku, jeśli to konieczne, należy sporządzić kopię danych zawartych na dyskach lub innych nośnikach danych. Następnie takie dane należy skutecznie usunąć, np. poprzez wielokrotne nadpisanie całych dysków lub ich fizyczne zniszczenie. Zabrania się przekazywania do utylizacji lub odsprzedaży sprzętu komputerowego zawierającego dane niejawne (w szczególności dane osobowe).

16.2.4. W przypadku podjęcia decyzji o programowym usunięciu danych, należy podjąć próbę ich odzyskania w celu zweryfikowania skuteczności zastosowanej metody.

16.2.5. W przypadku podjęcia decyzji o korzystaniu z usług firm zewnętrznych w procesie usuwania danych należy taki proces monitorować i potwierdzić jego skuteczność. Nie należy przekazywać sprzętu informatycznego w celu usunięcia danych poza miejsce ich przetwarzania.

16.3. Wycofywanie systemów informatycznych (oprogramowania)

16.3.1. Przed wycofaniem danego systemu informatycznego (oprogramowania) Administrator Systemu Informatycznego konsultuje się z osobami wykorzystującymi dane oprogramowanie w celu uzyskania pewności, że wycofywane oprogramowanie jest całkowicie zbędne.

16.3.2. Przed wycofaniem danego systemu informatycznego, należy zarchiwizować dane z wycofywanego systemu wraz z konfiguracją, oprogramowaniem i innymi narzędziami potrzebnymi do użycia w przypadku wystąpienia konieczności odwołania się do tych danych w przyszłości. Jeśli to konieczne należy zachować także wersje instalacyjne.

17. PRZEGLĄD I MONITOROWANIE SYSTEMÓW

Przeglądy systemów

17.1. ASI jest odpowiedzialny za nadzór nad działaniem zabezpieczeń i prawidłowym funkcjonowaniem systemu informatycznego, a w szczególności za:

1) weryfikację aktualności sygnatur systemu antywirusowego i podejmowanie ewentualnych działań korekcyjnych,
2) weryfikację logów systemu antywirusowego i podejmowanie działań korekcyjnych,
3) przegląd logów zapory sieciowej oraz podejmowanie działań mających na celu zablokowanie ataków sieciowych,
4) weryfikację poprawności aktualizacji oprogramowania systemowego.

17.2. Administrator Systemu Informatycznego przeprowadza okresowe przeglądy zainstalowanego oprogramowania w celu weryfikacji jego przydatności, aktualności. Oprogramowanie przestarzałe i nieprzydatne należy odinstalować.

17.2. Dziennik zdarzeń

17.2.1. Mechanizmy monitorowania i tworzenia dzienników zdarzeń powinny być stosowane w celu umożliwienia rejestracji działań związanych z bezpieczeństwem przetwarzania danych osobowych.

17.2.2. Dziennik zdarzeń powinien odzwierciedlać wymagania bezpieczeństwa przetwarzania danych osobowych. Zaleca się by jako domyślnie dziennik zdarzeń był przechowywany przez min. 6 miesięcy.

17.2.3. Dziennik zdarzeń powinien zawierać w szczególności:

1) identyfikator użytkownika, który wygenerował zdarzenie;
2) datę, czas i szczegóły ważnych zdarzeń, np. rozpoczęcia i zakończenia pracy w systemie;
3) pliki lub obiekty powiązane z wygenerowanym zdarzeniem;
4) adres IP źródłowy i docelowy;
5) zmiany konfiguracji systemu;
6) informację o zdarzeniu.

17.2.4. Zarejestrowane zdarzenia powinny być analizowane w celu identyfikacji problemów związanych z przetwarzaniem danych osobowych oceny skuteczności zaimplementowanych mechanizmów kontrolnych.

17.2.5. Dziennik zdarzeń należy zabezpieczyć przed modyfikacją oraz nieuprawnionym dostępem.

17.2.6. Zapisy w dziennikach zdarzeń należy regularnie przeglądać. Podczas przeglądu należy weryfikować ich integralność.

17.2.7. Dzienniki zdarzeń powinny bazować na poprawnym mechanizmie synchronizacji czasu.

18. NARUSZENIE BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

Użytkownik zobowiązany jest zawiadomić Administratora Danych Osobowych lub Administratora Systemu Informatycznego o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:

1) udostępnianiu osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych,
2) usiłowaniu logowania się do systemu informatycznego przez osobę nieuprawnioną,
3) użytkowaniu stacji roboczej przez osobę nie będącą użytkownikiem systemu informatycznego,
4) przebywaniu osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych,
5) pozostawianiu bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,
6) przechowywaniu nośników informacji lub wydruków z danymi osobowymi (które nie są przeznaczone do udostępniania) w warunkach umożliwiających do nich dostęp osobom nieuprawnionym,
7) naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła),
8) częściowym lub całkowitym braku danych lub ich nieuprawnionej modyfikacji,
9) dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
10) braku dostępu do właściwej aplikacji lub nietypowym działaniu aplikacji,
11) zmianie zakresu wyznaczonego dostępu do zasobów serwera,
12) wykryciu wirusa komputerowego,
13) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego,
14) znacznym spowolnieniu działania systemu informatycznego,
15) nietypowych komunikatach,
16) podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
17) zmianie położenia sprzętu komputerowego,
18) zauważeniu innych anomalii pracy komputera,
19) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.

Obowiązek dokonania zgłoszenia, o którym mowa powyżej spoczywa na każdym pracowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.

Do czasu przybycia na miejsce ADO lub ASI należy:

1) o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców,
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę.

ASI jest obowiązany niezwłocznie poinformować ADO o naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu.

ADO po otrzymaniu zawiadomienia powinien niezwłocznie:

1) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych, podjąć działania chroniące system przed ponownym naruszeniem,
2) w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego, a następnie niezwłocznie przekazać jego kopię ADO.
3) ADO w uzgodnieniu z Administratorem Systemu Informatycznego może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.

Administrator Systemu Informatycznego powinien podjąć następujące działania zmierzające do wyjaśnienia zgłoszonego zdarzenia w systemie informatycznym:

a) wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,
b) przeprowadzić wywiady z pracownikami w celu ustalenia zaistniałych faktów,
c) przeprowadzić analizę poprawności funkcjonowania systemu informatycznego w podmiocie, jeżeli zgłoszone zdarzenie było związane z nieprawidłowym jego funkcjonowaniem,
d) przeprowadzić analizę zapisu zdarzeń w systemie informatycznym z uwzględnieniem zapisu operacji realizowanych przez użytkowników,
e) przeprowadzić analizę danych przetwarzanych w systemie informatycznym, jeżeli zgłoszone zdarzenie mogło być spowodowane utratą dostępności lub integralności przetwarzanych danych,
f) zabezpieczyć dane przetwarzane w systemie informatycznym dotkniętym incydentem, w szczególności dane konfiguracyjne tego systemu,
g) zabezpieczyć system informatyczny przed dalszym rozprzestrzenianiem się zagrożenia,
h) zebrać materiały pozwalające na wyjaśnienie przyczyn zaistnienia incydentu, jego charakteru i potencjalnych skutków.
i) zasięgnąć potrzebnych opinii i zaproponować działania naprawcze (w tym także ustosunkować się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) oraz wznowienia terminu przetwarzania.

System informatyczny, którego prawidłowe działanie zostało odtworzone, powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu.

W czasie jej trwania użytkowanie systemu informatycznego powinno być ograniczone do niezbędnego minimum.

Okres obserwacji jest uzależniony od charakteru incydentu i specyfiki systemu informatycznego jest on każdorazowo określany przez Administratora Systemu.

W razie odtwarzania danych z kopii zapasowych administrator systemu obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu (dotyczy to zwłaszcza przypadków infekcji wirusowej).

ADO po zapoznaniu się z raportem, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego bądź zastosowaniu środków ochrony fizycznej.

ADO i ASI zobowiązani są do prowadzenia rejestru działania systemu informatycznego zawierającego informacje o:

1) awariach systemu informatycznego przetwarzającego dane osobowe,
2) wystąpieniu istotnych zagrożeń dla działania systemu informatycznego
3) zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami,
4) nieprzestrzeganiu zasad używania oprogramowania antywirusowego,
5) niewłaściwym wykorzystaniu sprzętu komputerowego lub przetwarzaniu danych w sposób niezgodny z procedurami ochrony danych osobowych.

19. POSTANOWIENIA KOŃCOWE

19.1. Instrukcja Zarządzania Systemem Informatycznym stanowi wewnętrzną regulację ADO i obowiązuje wszystkich pracowników i współpracowników ADO. Instrukcja obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u ADO. Wszelkie zmiany w Instrukcji obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty u ADO.

19.2. Użytkownicy systemu zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Instrukcji, w wypadku odrębnych od zawartych w niniejszej Instrukcji uregulowań występujących w innych procedurach obowiązujących w Urzędzie użytkownicy systemu mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych przetwarzanych w systemie informatycznym.

19.3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.

19.4. W sprawach nieuregulowanych w Instrukcji zarządzania Systemem Informatycznym mają zastosowanie przepisy powszechnie obowiązującego prawa w szczególności przepisy rozporządzenia RODO, Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. 2018 poz. 1000) oraz przepisy wykonawcze do tej Ustawy.

Zapisy tego dokumentu wchodzą w życie z dniem 2 listopada 2021 r.

Administrator Danych Osobowych: *Związek Gmin Krajny w Złotowie,*

ul. Wawrzyniaka 4a, 77-400 Złotów

Administrator Systemu Informatycznego: *Marcin Grobelny, prowadzącym działalność gospodarczą pod firmą MAXIMUS CENTRUM KOMPUTEROWE Marcin Grobelny*

Inspektor Ochrony Danych Osobowych: *Marcin Misztal*

Administrator Systemu Informatycznego:	**Administrator Danych Osobowych:**
……..	……..
Data, podpis i pieczątka	Data, podpis i pieczątka

ZAŁĄCZNIKI:

Załącznik nr 1 - „Regulamin użytkownika systemu informatycznego”

Załącznik nr 2 - „Wniosek o nadanie, modyfikacje, odebranie uprawnień”

Załącznik nr 3 – „Rejestr uprawnień do systemów informatycznych”

Załącznik nr 4 - „Rejestr tworzenia kopii”

Załącznik nr 1 *do Instrukcji Zarządzania Systemem Informatycznym*

„Regulamin użytkownika systemu informatycznego”

1. Użytkownik systemu informatycznego zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą Dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji, regulaminami i instrukcjami wewnętrznymi.
2. Użytkownik zobowiązany jest do ochrony danych systemu informatycznego przed dostępem osób nieupoważnionych.
3. Użytkownik zobowiązany jest do ochrony danych systemu informatycznego przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją.
4. Użytkownik chroni nośniki danych oraz wydruki komputerowe przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem.
5. Obowiązkiem użytkownika jest utrzymywanie w tajemnicy powierzonych identyfikatorów, haseł, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia.
6. Użytkownik archiwizuje dane zgodnie z instrukcją.
7. Użytkownik obsługujący system informatyczny w obszarze przyznanego mu dostępu do systemu zobowiązany jest do sprawdzania czy nie wprowadzono nieautoryzowanych aplikacji oraz zmian w zainstalowanych aplikacjach.
8. Zabrania się pod rygorem odpowiedzialności służbowej i karnej ujawniania danych, kopiowania baz danych lub ich części poza przewidzianymi kopiami zapasowymi.
9. Zabrania się wykorzystywania sprzętu komputerowego i sieci komputerowej do celów prywatnych.
10. Zabrania się używania prywatnych komunikatorów.
11. Zabrania się ściągania i wysyłania plików (filmów, muzyki itp.) niezwiązanych z obowiązkami zawodowymi.
12. Zabrania się korzystania z nośników nieznanego pochodzenia.
13. Zabrania się instalowania jakiegokolwiek oprogramowania bez wiedzy ASI.
14. Dopuszcza się wykorzystanie zarejestrowanych pamięci pendrive lub innych nośników do przenoszenia informacji wewnątrz siedziby jednostki, a także za zgodą i wcześniejszym sprawdzeniem nośnika przez administratora sieci, poza siedzibę w ściśle określonym celu.
15. W celu zachowania bezpieczeństwa wszelkie dane indywidualne i funkcyjne przechowywane są na dyskach lokalnych komputerów użytkowników, zaś kopie na dyskach sieciowych w lokalnej sieci komputerowej.
16. Zaleca się robienie kopii zapasowych ważnych plików i baz danych, jeśli nie są realizowane centralnie. Kopie należy wykonywać na udziałach sieciowych.
17. Użytkownik jest zobowiązany do zachowania porządku na biurku w trakcie pracy oraz zabezpieczenia wszystkich dokumentów po jej zakończeniu.
18. Użytkownik jest zobowiązany do stosowania zasady „czystego pulpitu” polegającej na blokowaniu stacji poprzez wciśnięcie równocześnie klawisza „Windows” + „l”.
19. Wszelkie niepotrzebne wydruki - dokumenty/brudnopisy należy zniszczyć w niszczarce jeśli zawierają dane osobowe, pieczątki firmowe, podpisy itp.; zabrania się wyrzucania całych dokumentów do śmietnika.

Załącznik nr 2 *do Instrukcji Zarządzania Systemem Informatycznym*

WNIOSEK O NADANIE/MODYFIKACJĘ/ODEBRANIE UPRAWNIEŃ DLA UŻYTKOWNIKA W SYSTEMIE INFORMATYCZNYM

Nowy użytkownik	Modyfikacja uprawnień	Odebranie uprawnień w systemie

DOTYCZY SYSTEMU: ……

nazwa systemu/rodzaj konta

Imię i nazwisko użytkownika:		
Jednostka Organizacyjna/Dział:		
Posiada upoważnienie do przetwarzania danych osobowych:	TAK	NIE
Opis zakresu uprawnień użytkownika w systemie informatycznym i uzasadnienie:		
Data obowiązywania uprawnienia:		
Data zgłoszenia:	**Podpis Administratora Danych Osobowych:**	

Załącznik nr 3 *do Instrukcji Zarządzania Systemem Informatycznym*

REJESTR UPRAWNIEŃ DO SYSTEMÓW INFORMATYCZNYCH						
Lp.	Imię i nazwisko osoby uprawnionej	Data nadania uprawnienia	Data ustania uprawnienia	Nazwa systemu/usługi/udziału	Identyfikator/login	Osoba odpowiedzialna
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Załącznik nr 4 *do Instrukcji Zarządzania Systemem Informatycznym*

REJESTR TWORZENIA KOPII								
Lp.	Nazwa kopiowanego systemu/aplikacji	Nazwa serwera /komputera	Rodzaj kopii: obraz systemu, baza danych, pliki, poczta, inne.	Typ kopii: pełny, przyrostowy, różnicowy.	Wolumen (GB)	Miejsce przetrzymywania kopii (np. dysk zewnętrzny, nośniki CD/DVD, inne)	Data utworzenia kopii	Osoba odpowiedzialna
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								